Information Security
What You Need to Know

July 2005

Definition

Protect CDC's Information Assets From **Unauthorized**

- Access
- Modification
- Disclosure
- Deletion

Law and Policy

- Information Practices Act (CC, § 1798)
- Public Records Act (CC, §§ 6250-6265)
- Records Management Act
  (GC §§ 14740-14770)
- Penal Code § 502
- SAM, Sections 4840 through 4845
- DOM, Articles 45 through 48

Local ISC/PcAdmin Role

- Record Keeping
- Coordinate Awareness Training
- Ensure Compliance
- Oversee Inmate Use of Computers
- Report Information Security Incidents
- Installations
- Local Operational Recovery Planning.

Record Keeping

- Inventory and Asset Management
- Software Licensing and Usage
- Account Management
- User Agreement Forms.

Record Keeping
Inventory and Asset Management

- Computers and Peripherals
- Software Usage
- Handhelds and PDAs
- Modems
- Maintenance and Repair
- Network Diagrams
- Inmate Computers.

Record Keeping
Account Management

- Know Who is Using What
- Internet Access
- Delete Old Accounts
- Global Address Book.

Record Keeping
User Agreement Forms

- CDC 3025
- CDC 1857
- CDC 1900

Awareness Training

- Annually
- Employee Awareness Handbook
- Online Quiz with Certificate
- Training Coordinator maintains the Records.

Ensure Compliance

- Staff Adherence to password/logon policy
- File Transfers
- Inmate (offender) Access
- Backups on designated systems

Ensure Compliance
Confidential and Sensitive Data

- Level of Protection Must be Maintained
- Removing Data from Workplace (DOM 13030.30)
- Personal Information (CC 1798.29)

Ensure Compliance

Audits, Logs and Scans

- Centralized CDC Network Management
- Application Security
- Internet Access
- Email Usage
- Self- Assessments and Security Audits

Inmate Access to Computers

- CCR, Title 15, Section 3041.3
- DOM, Section 42020.6
- DOM, Sections 49020.18 - 49020.18.7

Inmate Access to Computers

- Signage
- Utilities and Operating Systems
- Networks
- Inmates and Staff
- Work and Education Assignments
- Supervision
- Converting Staff Computers to Inmate Use

Inmate Access to Computers

- Removable Media
- Peripheral Devices
- Software and Development Tools
- Modems
- Inmate-Developed Applications
- Authorization for Inmates on Computers

Information Security Incidents

- All incidents reported through chain of command and to the ISO
- Within three days of becoming aware of the incident
- Reporting template at intranet/information security.

Information Security Incidents

- Inmates using Computers in unauthorized manner
- Inmates in possession of confidential or personal information
- Unauthorized Access to Information Systems
- Defacement of Web Pages
- Denial of Service Attacks
- Lost or Stolen Computers, including Laptops and PDAs.

Installations

Malicious Code – Viruses, Worms other Slugs

- McAfee on CDC Network
- Non-Networked Computers
- Inmate Use Computers
- Protecting Our Systems and Data.

Installations
Software and Patches

- “Standard” Applications
- “Non-Standard” Applications
- Incorporate into Images
- Updates, New Versions and Patches.

Operational Recovery

- Business Resumption
- Why This Is Necessary
- Critical Applications
- Restore Location
- Backup Availability
- Resource Requirements
- Testing the Plan.

Resources

- Intranet/Infosec
- Intranet/RPMB
- sam.dgs.ca.gov/TOC
- www.leginfo.ca.gov
- www.ohi.ca.gov
- www.cert.org

Questions